ABSTRACT

A process is provided for searching in parallel for a plurality of prime number values simultaneously includes the steps of: randomly generating a plurality of k random odd numbers (wherein k is preferably more than 2, but could also be one or more) expressed as $n_{0,0}$, $n_{1,0}$, ... $n_{((k-1)),0}$, each number providing a prime number candidate; determining a plurality of y additional odd numbers based on each one of the randomly generated odd numbers $n_{0,0}$, $n_{1,0}$, ... $n_{(k-1),0}$ to provide additional prime number candidates thereby yielding a total number of prime number candidates; sieving the total number of prime number candidates by performing a small divisor test on each of the candidates in order to eliminate candidates revealed to be composite numbers by the small divisor test thereby yielding a sieved number s of candidates; and performing a first probabilistic primality test on each of the sieved number s of candidates, each of the plurality of s first primality tests including an associated exponentiation operation executed by an associated one of a plurality of s of the exponentiation units, the exponentiation operations being performed by the plurality of s exponentiation units substantially simultaneously in order to eliminate candidates revealed to be composite numbers by the primality test thereby yielding a remaining number r of candidates.